

# QR Code as Private Key on El Gamal Algorithm

Ridho Akbarisanto - 13511005  
Program Studi Teknik Informatika  
Sekolah Teknik Elektro dan Informatika  
Bandung, Indonesia  
ridho.akbarisanto@yahoo.com

**Abstract**—In this paper one of the alternative ways to find the private key on El Gamal algorithm. The proposed way to achieve the goal is by using the QR Code to generate the private key and the public key. QR Code has the needed structure that fit into this problem. In this paper the implementation will be in Java programming language using Eclipse tool.

**Keywords**—Elgamal; Modern Cryptography; private key; QR Code.

## I. INTRODUCTION

Communication is the act or process of using words, sounds, signs, or behaviors to express or exchange information or to express your ideas, thoughts, feelings, etc., to someone else. Communication is a way used by creature to interact with other creatures. Different creatures have their own ways to communicate. Plants have their own ways to communicate with other plants, animals can use gesture and sound to communicate with other animals, and like animals, people can use gesture and sound, and also many other ways to communicate. Sometimes people can also just use sign to communicate with others.

Everything in this world is changing, including communication. In the beginning, the communication can be done just by meeting with other persons, using gesture or speaking. And then people don't have to meet another person to communicate, even when the persons communicating are on a long distance. At first the long distance communication can be done by sending letters using pigeon as the courier. This communication needs a lot of time, and then human found the alternative. The alternative way is using the people itself to send the letters, because the discovery of vehicle. It takes less time than using pigeon. And then the need of the distance and time is increasing for people, because people can go to another country using vehicles. Then the inventions of the telephone make it easier to communicate in a long distance communication. Everybody can talk using telephone to anybody having telephone in another place. People keep developing the technology, including the phone. The discovery of cell phone makes it a lot easier to communicate, by using short message service or by calling. And then it keeps developing. The internet service become easier to access, and because of that the messenger or chat technology is used and even video call. And it will keep changing and changing to another form. It will keep happening because the need of the people is increasing every day.

The changes of the communication form to distance communication bring out many other problems, like "how do we know that we really send the messages to the receiver and get the messages from the same sender?" or "how do we know that the communication is not being hijacked by another person?". People then think the solution of these problems that is as long as the receiver gets the meaning, the process of the communication can be modified. The modifying process is what people do in cryptography so the one that understands the message are just the sender and the receiver of the message.

In classic cryptography, the message that people use is often in physical form, like writing on a paper, so the methods used for the modifying process are substitution and transposition. In modern cryptography, the message that people use is in digital form, usually in computers. The substitution and transposition still can be used, but they are not effective enough to secure the messages. The algorithm for the modern cryptography involves the bit operation of the messages bits. One of the algorithms is using private and public key. The private and public keys are using 2 different big number values. Because of the big number, people often forget about the numbers. There are many ways to solve the problems. The proposed way to solve the problem is by using QR code.

QR (Quick Response) code is a two dimensional code first created by a company in Japan. QR code can store any contents from text to URL. But in this paper the contents are not exactly needed. QR code is unique one to another. The uniqueness of the QR code is in the structure of the QR code. The only thing needed is to process the elements of the QR code so it can be used as the private key on the elliptical curve algorithm. By using the QR code, the expected output is as good as the usual algorithm.

## II. THEORY

### A. El Gamal Algorithm

El Gamal is one of the modern cryptography algorithms which uses public and private keys. In this algorithm there are several values that needs to be decided by the sender and receiver of the messages, which are  $p$ ,  $g$ ,  $x$ ,  $y$ ,  $m$ ,  $a$  and  $b$ .

$p$  is a big prime number which can be shared to anyone publicly because it's useless to know the public key if the people don't have the private key.  $g$  is a random positive number which is less than  $p$ . Like  $p$ , everyone can know the

value of  $g$ .  $x$  is also a random positive number which is less than  $p$ . The difference between  $g$  and  $x$ ,  $x$  must be kept secret because  $x$  is the private key.  $y$  is the public key of this algorithm which can be found using this equation :

$$y = g^x \text{ mod } p$$

$m$  is the value of the message that needs to be encrypted and  $m$  is secret. And then  $m$  will be encrypted to value  $a$  and value  $b$  using the private key.

There are several processes in the ElGamal algorithm. The processes are like below.

1. Find the value of  $p$
2. Find a random value of  $g$ , less than  $p$
3. Find the random value of  $x$  with the rule,  $1 \leq x \leq p-2$
4. Find  $y$  by using the equation earlier.

After the steps above, then the public key is obtained, which are  $p$ ,  $g$ , and  $y$  and the private key which is  $x$ . After that the next step is to do the encryption and decryption of the messages.

The steps need to be done for encrypting the message will be explained below.

1. Align the message  $m$  to several blocks which is for every block is in the range of 0 and  $p-1$
2. Find a random value  $k$  which is in the range of  $1 \leq k \leq p-2$
3. Each block then needs to be encrypted using the equation  $a = g^k \text{ mod } p$  and  $b = m \cdot g^k \text{ mod } p$ .

And the decryption of the message will also be explained below.

1. Using the private key  $x$ , find the value of  $(a^x)^{-1} \text{ mod } p$
2. Find message blocks  $m$  using equation  $m = b/a^x \text{ mod } p = b(a^x)^{-1} \text{ mod } p$

### B. QR Code

QR code is two-dimensional code which is categorized in matrix code. QR code (Quick Response code) is first used for the automotive industry in Japan. QR code is similar to barcode, but QR code is able to store bigger data than barcode because it can store informations vertically and horizontally. QR code is also included in cryptography because it uses 56 bit DES algorithm.

QR code has an unique structure. The structure consists of five major components with each different functions.

#### 1. Finder Pattern

The pattern is used for detecting the position of the QR code. It has three identical square boxes located at the upper right, upper left, and lower left corners of the QR code.

#### 2. Alignment Pattern

The patter in used for correcting the distortion when the scanning process of the QR code is running.

#### 3. Timing Pattern

The pattern consists of the horizontal and vertical parts. The vertical part goes from the right side of the lower left finder pattern to the right side of the upper left finder pattern, and the horizontal part goes from the lower side of upper left finder pattern to the lower side of upper right finder pattern. The pattern actually consists of a one module wide row or column of alternating dark and light modules.

#### 4. Quiet Zone

This component is like a margin space of the QR code. It surrounds the symbol on all four sides to make the symbol detection easier.

#### 5. Data Area / Encoding Region

The region is the place where the data stored. Data is encoded into binary value 0 and 1 based on some rules. The white module represents 0 and the black module represents 1. The area also consists of version information, format information, and error correction codewords.

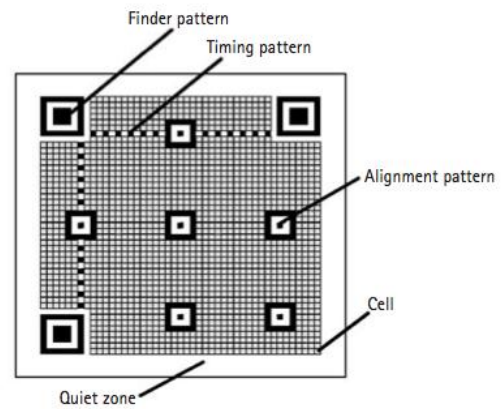


Figure 1 Structure of QR code

There are four kinds of characters which can be encoded in QR code, numeric, alphanumeric, 8bit byte data, and KANJI. The numeric consists of 10 characters (0-9) and 3 characters are encoded to 10bit length. The alphanumeric consists of 45 characters (0-9A-Z\$%\*+-./:) and 2 characters are encoded to 11bit length. KANJI character is encoded to 13bit length.

QR code has an error correcting function for misreading the white color for black color. There are four level of correction as below.

1. Level L (Low) : About 7% or less can be corrected.
2. Level M (Medium) : About 15% or less can be corrected.
3. Level Q (Quartile) : About 25% or less can be corrected.

4. Level H (High) : About 30% or less can be corrected.

There are many sizes of QR code. The size of QR code is defined as version. There are 40 versions of QR code. Version 1 is 21\*21 matrix and version 40 is 177\*177 matrix. For each 1-level increasing, the size will increase by 4.



Figure 2 Version 1 of QR code

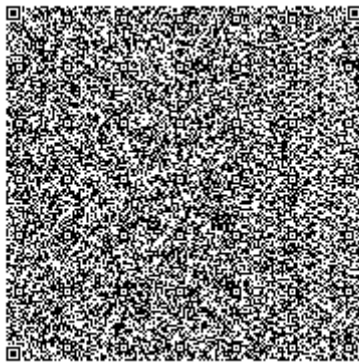


Figure 3 Version 40 of QR code

### III. DESIGN

The main concern of this paper is to find the alternative of finding the private key and the public key for communication by exchanging messages, so the messages will stay hidden for anyone else except the communicator who got the keys. This should be done because people often forget about the keys which are usually a big number and sometimes people forgot to save it or even people misses the key. There are also many uses of the texts for generating the keys, but with just text then it also can't be so secured because people can know the text too. The proposed way is to use the QR code to generate the keys, because QR code has many advantages in it. It has several elements that can be used like finder pattern, alignment pattern, timing pattern, quiet zone, and the data area. It is also unique from one to another QR code. And people don't have to remember the QR code because there are already many QR code generators which can be used easily.

The difference between the proposed algorithm and the usual ElGamal algorithm is in the process of getting the points to generate the keys. In this algorithm, the QR code image needs to be processed first to get the points. Not all of the components of the QR code will be used to generate the points. The quiet zone and the finder pattern won't be used because each QR code has that so it can be used to distinguish one with another. There are two kinds of QR codes, dynamic and static. The one that will be used in this paper is the static QR code.

In this paper, the testing done by creating a simple program which can input the QR code as the key of the El Gamal algorithm, also it can encrypt and decrypt the message using the key generated before. The program will be created using Eclipse tool and Java programming language.

### IV. IMPLEMENTATION

The implementation, as described previously above, will be created using Eclipse tool and Java language. The implementation consists of three major processes, the image processing which will convert the QR code image to get the list of points in the equation, the generation of the public and private keys using the points, and the main process to encrypt or decrypt the messages.

#### A. Image Processing

The first process of the implementation is processing the QR code image. The process is done to generate the parameters needed for the key generation, the points of the equation. The image processing won't be too difficult because there are just two colors in the QR code image, black (with RGB 0 0 0) and white (with RGB 255 255 255). The process will be done by iterating the image from upper left to the lower right to check the each module in the QR code.

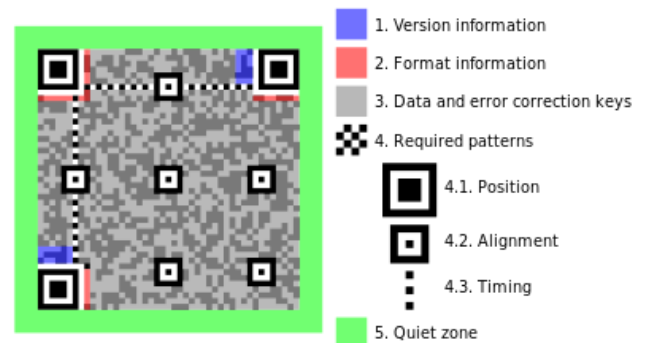
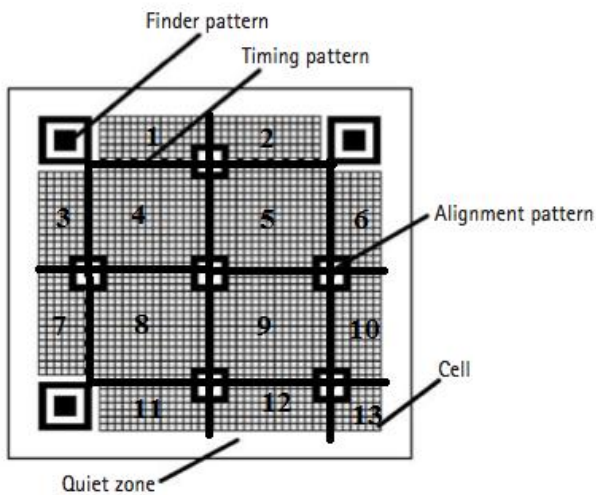


Figure 4 QR Code structure

But before the process is done, as mentioned before, the quiet zone and the finder pattern won't be included in the process. Then the other elements, like version information and format information will be noted to find the points for key generation.

After that, using the alignment and the timing patterns, the QR code can be divided into several parts. For the experiments the QR code image will be divided into 13 parts of image.



**Figure 5 Divided parts of QR Code**

Then for each parts of the data area the process needed is to find the point from the data area.

```
for (int i = 0; i < qrParts.length; i++) {
    QRParts qrNow = qrParts.get(i);
    partToPoint(qrNow.x,qrNow.y,qrNow.width,qrNow.height
);
}
```

Then the next problem is how to find the point from the part. In this experiment the number of the black cell in each parts will be counted. The total number of the black cell then will be computed with the version and the format information already been found before.

After the process, the result will be 13 different points. All the different points then will be used in the next process, key generation. The 13 different points are different from one QR code to another QR code.

### B. Key Generation

The key generation will be based on El Gamal algorithm. There are two kinds of key that should be generated, the public key and the private key. For the public key, the triplet values (y, g, and p) are needed and the pair values (x and p) for the private key. Unlike usual process of key generation, the first value that needed to be found is x, the private key. The method that will be used to find x is simple, just by combining all of the points got from before into long-string represents big integer.

```
String xTmp = "";
for (int i = 0; i < points.length; i++) {
    xTmp = xTmp + point.get(i).getX().toString() +
points.get(i).getY().toString();
}
```

```
}
BigInteger x = new BigInteger (xTmp);
```

After getting the value of x, then the next step is to find the prime number p which is bigger than x.

```
BigInteger p = new BigInteger(randomBigInt().toString());
while (!isPrime(p) || !isBigger(x,p)) {
    p = new BigInteger(randomBigInt().toString());
}
```

After the process above, the pair values of private keys found, Then the next step is to find the triplet values for the public key. The process below is to find the next number, g, which is different to p and less than p.

```
BigInteger g = new BigInteger(randomBigInt().toString());
while (!isLess(g,p)) {
    g = new BigInteger(randomBigInt().toString());
}
```

The last process in the key generation is to find the y value using the equation  $y = g^x \text{ mod } p$ .

```
BigInteger y = modulo(power(g,x),p);
```

### C. Encryption and Decryption

After getting the private key and the public key, the standard encryption and the decryption using ElGamal algorithm will be done. The process will start with finding the value of a n b, which will represents the ciphered text but not the final original message.

```
for (int i = 0; i < mBlocks.length; i++) {
    BigInteger k = new BigInteger(randomBigInt().toString());
    while (!isLess(k,P)) {
        k = new
        BigInteger(randomBigInt().toString());
    }
    BigInteger a = modulo(power(g,k),p);
    BigInteger b = modulo(power(y,k),p);
    cipheredA.add(a);
    cipheredB.add(b);
}
```

The encryption process considered done when the two ciphered text got. The size of the ciphered text so will be bigger twice than the original size.

The decryption process will convert the ciphered text a and b into the original message using the private key x. The last step is to combine the message blocks to build the original message with original message size.

```
for (int i = 0; i < cipheredA.length; i++) {  
    BigInteger aix = cipheredA.get(i).getX();  
    message = message + cipheredB.get(i).process(aix);  
}
```

## V. ANALYSIS

From the experiments done, the result is corresponding to the expected output. The public and private keys generated from the image processing can be used to encrypt the messages using the elgamal algorithm. The decryption also can be done well using the same keys. The points generated from the image processing of QR code are good enough to use as the parameters of the equation. The image processing is also not too difficult to implement because the elements of the QR code is not too complex. The future works will be to integrate this with bigger area of work.

## VI. CONCLUSIONS

The private and public key generation using QR Code is possible to be done. The process needs to achieve the goal is not too complex and it's easy to implement. The QR code can be got using many tools already been created. The proposed algorithm is fit to solve many problems in modern cryptography, especially in public-private key algorithm.

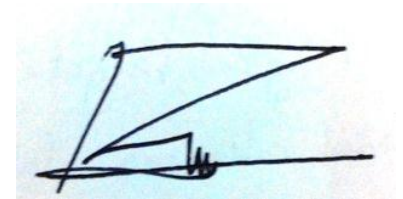
## REFERENCES

- [1] [http://www.swetake.com/qrcode/qr1\\_en.html](http://www.swetake.com/qrcode/qr1_en.html) diakses pada tanggal 10 Mei 2015.
- [2] <https://blogs.commons.georgetown.edu/cctp-797-fall2013/archives/838> diakses pada tanggal 10 Mei 2015.
- [3] <http://www.merriam-webster.com/dictionary/communication> diakses pada tanggal 10 Mei 2015.
- [4] Taher ElGamal (1985). "A public key cryptosystem and a signature scheme based on discrete logarithm". *IEEE Transactions on Information Theory* 31 (4): 469-472.

## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 11 Mei 2015



Ridho Akbarisanto

13511005